REMARKS/ARGUMENTS

This application has been carefully considered in connection with the Examiner's Final Office Action dated July 13, 2006. Reconsideration and allowance are respectfully requested in view of the following.

Summary of Rejections

Claims 1-24 were pending at the time of the Office Action.

Claim 1-24 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Blakley, III et al. (U.S. Patent No. 5,832,211, "Blakley") and further in view of Mehring et al. (U.S. Patent No. 6,609,115, "Mehring").

Summary of Response

Claims 1-24 remain as originally submitted or previously presented.

Remarks and Arguments are provided below.

Summary of Claims Pending

Claims 1-24 are currently pending following this response.

Response to Arguments

The Office Action responded to Applicants' arguments filed on April 24, 2006, as follows:

1. The actions of converting unencrypted data to be compatible with target data store and populating target data store with the converted data are not "nonfunctional descriptive material".

The Office Action suggested that the actions recited in Claim 1 of converting unencrypted data to be compatible with target data store and populating target data store with the converted data are only found in the nonfunctional descriptive material and are not functionally involved in the actions recited. However, Applicants respectfully submit that the Interim Guidelines for Examination of Patent Applications for Patent Subject Matter Eligibility published in the Official Gazette Notices on November 22, 2005, define "nonfunctional descriptive matter" as follows:

> Descriptive material can be characterized as either "functional descriptive material" or "nonfunctional descriptive material." In this context, "functional descriptive material" consists of data structures and computer programs which impart functionality when employed as a computer component. (The definition of "data structure" is "a physical or logical relationship among data elements, designed to support specific data manipulation functions." The New IEEE Standard Dictionary of Electrical and Electronics Terms 308 (5th ed. 1993).) "Nonfunctional descriptive material" includes but is not limited to music, literary works and a compilation or mere arrangement of data.
>
> ... When functional descriptive material is recorded on some computer-readable medium it becomes structurally and functionally interrelated to the medium and will be statutory in most cases since use of technology permits the function of the descriptive material to be realized.

In light of the guidelines above, Applicants respectfully submit that that the actions of converting unencrypted data to be compatible with target data store and populating target data store with the converted data are not "nonfunctional descriptive material". These actions are positively recited in Claim 1. Therefore, Applicants respectfully request that all of the claim

limitations of Claim 1 be considered in determining patentability.

2. Mehring does not eliminate the need to submit the user information to the authenticator once the user information is in the cache.

In response to Applicants' submission that Mehring does not disclose submitting the received identification and received password to the source user authenticator **if** the target data store does not include a password associated with the identification, the Office Action suggested that Col. 10., line 49 – Col. 11, line 10 of Mehring teaches submitting the received identification and received password to the source user authenticator if the target store does not include a password associated with the identification.

However, the cited section of Mehring teaches that although the remote user is only required to log-in once, the user information stored in the web browser log-in cache is still submitted to the policy server **every time** the remote user logs-in to a different web server. Therefore, Mehring does not eliminate the need to submit the user information to the authenticator once the user information is in the cache. It only eliminates the need of having the remote user log-in separately to different web servers. The received identification and password are still submitted to the source user authenticator every time the remote user logs-in to a different web server even though the information is already in the browser log-in cache. By contrast, with the present application, the received identification and password are only submitted to the source user authenticator if they are not in the target datastore. Once they are in the target datastore, they are no longer submitted to the source user authenticator for authentication.

3. Applicants are unable to find any teaching or suggestion in any of the cited references to make the suggested modification of intercepting a request to the source user authenticator from a user seeking access to information protected by the target user authenticator.

In response to Applicants' submission that the cited references do not teach or suggest intercepting a request to the source user authenticator from a user seeking access to information protected by the target user authenticator, the Office Action suggested that it would have been obvious to one having ordinary skill in the art to if the target data store does not include a password associated with the identification, then submit the received identification and received password to the source user authenticator since it is known in the art that during a data base migration period, if the target data store does not include a password associated with the identification, then submit the received identification and received password to the source user authenticator.

However, Applicants respectfully submit that the teaching or suggestion to make the claimed modification must be found in the prior art and not based on Applicants' disclosure. Applicants are unable to find any teaching or suggestion in any of the cited references to make the suggested modification.

In migrating from one datastore to another, the non-encrypted data is migrated from the first authenticator's datastore to the second authenticator's datastore. This will include the roles, resources, and user information (except password). The passwords can not be migrated in this fashion because they are stored in a proprietary encryption algorithm. As stated in Paragraph [0018] of the present disclosure, one of the most difficult aspects of migration of an authentication system is migration of the authentication information for the individual users (whether the users are persons or applications or other computers or networks). While one could

always simply change out the authentication system and have every user re-register to provide new security information this involves substantial coordination including safeguards that the authorized user is the one providing the new information. It also causes significant additional effort by the end users, while a more transparent migration reduces end user frustration. Finally, in a simple world one could replicate or transform the security datastore to a datastore for the new system, porting the information across all at once and having it available for the new authenticator to use. However, as discussed in the application, the custom nature of some of the schema and the various encryption efforts make this task highly challenging to impossible for some migrations.

Therefore, what is needed is a method and system for migrating authentication information from one database to another in a manner that is as transparent to the end user as reasonably possible. The present application solves this problem by querying the new datastore to determine if a user who has logged in has a password in the new datastore (which in this case would mean that the user has not used the system since the migration). If the user does not have a password in the new datastore, the user will be forwarded to the access server to receive the login page from the old authenticator. As the user enters their password within the access server's login page, a password capture process (referred to in the vernacular as a sniffer) piggy-backed onto the access server will capture (or sniff) the raw password. The captured password is then entered into the new datastore where it will be used to authenticate the user at every subsequent log-in.

Thus, the obvious ways of migrating data from one datastore to another are to either have the users re-register by providing new security information or port the information across all at once and have it available for the new authenticator to use. It is not by intercepting a request to

the source user authenticator from a user seeking access to information protected by the target user authenticator.

For the reasons established above, Applicants respectfully submit that the arguments previously submitted on April 24, 2006, have not been traversed and continue to distinguish the present application from the cited references. Accordingly, Applicants respectfully resubmit the following arguments:

Response to Rejections under Section 103

In the Final Office Action dated July 13, 2006, Claim 1-24 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Blakley, III et al. (U.S. Patent No. 5,832,211, "Blakley") and further in view of Mehring et al. (U.S. Patent No. 6,609,115, "Mehring").

I. Blakely does not teach or suggest a method for migrating from a source user authenticator to a target user authenticator that locates a corresponding identification in a target datastore and determines whether the target datastore includes a password associated with the identification.

Claim 1 recites, "A method for migrating from a source user authenticator ... to a target user authenticator ... comprising ... Locate the corresponding identification in the target datastore and determine whether the target datastore includes a password associated with the identification."

The Office Action appears to suggest that the foreign registries of Blakely locate a corresponding identification in their target datastore and determine whether their datastores include a password associated with the identification. However, Applicants are unable to find such a teaching in Blakely. The section of Blakely cited in support of this suggestion (Col. 11, lines 44-55) describes the requirements met by the password synchronization function. The requirements do not include locating a corresponding identification in their target datastore and determining whether their datastores include a password associated with the identification. It is

not necessary for the foreign datastores of Blakely to determine if their datastores include a password associated with an identification because they are networked with the main data store. Their datastores are configured to be propagated immediately with any changes to passwords in the DCE datastore. Col. 11, lines 27-32 of Blakely states:

> ... synchronization causes passwords changed by DCE users to be propagated as plaintext passwords **to any** other foreign registry configured to receive such changes. **Propagation is immediate**, with results saved for retry, as necessary, should communications with the foreign registries be broken. (Emphasis added by Applicants.)

Therefore, no determination is made by the foreign registries. They simply receive any changes made to the DCE passwords.

More importantly, simply propagating passwords from one datastore to another is not what is claimed and can be highly challenging to impossible when migrating from one vendor's proprietary database schema to another vendor's product. While one could always simply change out the authentication system and have every user re-register to provide new security information, this involves substantial coordination including safeguards that the authorized user is the one providing the new information. It also causes significant additional effort by the end users, while a more transparent migration reduces end user frustration. Finally, in a simple world one could replicate or transform the security datastore to a datastore for the new system, porting the information across all at once and having it available for the new authenticator to use. However, as discussed above, the custom nature of some of the schema and the various encryption efforts make this task highly challenging to impossible for some migrations.

In response to these difficulties, the present application discloses a desirable feature in a security migration to port user data out of the proprietary and/or encrypted datastore of the old authenticator and into the new datastore for the new authenticator while minimizing the impact on the user experience, thereby allowing transitioning from one authenticator to the next for the protection of web resources with minimal impact to applications or users. Blakely does not address the problems associated with migrating data from one vendor's proprietary database schema to another vendor's product and does not teach or suggest the solution disclosed in the present application.

Accordingly, Applicants respectfully submit that Blakely does not teach or suggest a method for migrating from a source user authenticator to a target user authenticator that locates

the corresponding identification in the target datastore **and determines whether the target datastore includes a password associated with the identification**.

II. Mehring does not teach or suggest a method for migrating from a source user authenticator to a target user authenticator that submits the received identification and received password to the source user authenticator if the target datastore does not include a password associated with the identification.

Claim 1 also recites, "A method for migrating from a source user authenticator ... to a target user authenticator ... comprising ... If the target datastore does not include a password associated with the identification, then submit the received identification and received password to the source user authenticator."

The Office Action appears to suggest that the authentication step described in Mehring discloses submitting the received identification and received password to the source user if the target data store does not include a password associated with the identification. However, as stated earlier, Mehring does not teach or suggest a method for migrating from a source user authenticator to a target user authenticator. Instead, Mehring describes a method for allowing a remote system user to requests multiple software applications using a single log-in. More importantly, as stated in the section of Mehring cited in the Office Action (Col. 10., line 49 – Col. 11, line 10), although the remote user is only required to log-in once, the user information stored in the web browser log-in cache is submitted to the policy server every time the remote user logs-in to a different web server. Therefore, having user information stored in the web browser log-in cache does not eliminate the need to submit the user information to the policy server every time the remote user logs-in to a different web server. It only eliminates the need of having the remote user log-in separately to different web servers. By contrast, in the present application, once a password is associated with an identification in the target datastore, there is no longer a need to submit the request to the source user authenticator.

Accordingly, Applicants respectfully submit that Mehring does not teach or suggest a method for migrating from a source user authenticator to a target user authenticator that submits the received identification and received password to the source user authenticator if the target datastore does not include a password associated with the identification.

III. The system and method of the present application populates the target datastore with the received password from the user. It does not populate the target datastore with the password from the source user authenticator.

Claim 1 further recites, "A method for migrating from a source user authenticator ... to a target user authenticator ... comprising ... On receipt of an approval response from the source user authenticator, populate the target datastore with the received password associating the received password with the corresponding identification."

The Office Action noted that Blakely does not disclose this element. However, the Office Action suggested that:

> It would have been obvious to one having ordinary skill in the art at the time of the invention was made to on receipt of an approval response from the source user authenticator populate the target datastore with the received password associating the received password with the corresponding identification, since it is known in the art to facilitate the complete transfer of data, when data is found missing from the original source, it is restored by the data from the original source. (Page 5.)

Applicants are unclear as to how data can be restored from the original source if it is missing from the original source. If the Office Action is suggesting that the target datastore of the present application is populated with passwords from the source datastore, Applicants respectfully submit that this understanding incorrectly reflects the claimed subject matter. The claims calls for using the received password (received from the User) to populate the target datastore. For the reasons stated earlier, the target datastores cannot be populated with passwords from the source datastore because simply propagating passwords from one datastore to another can be highly challenging to impossible when migrating from one vendor's proprietary database schema to another vendor's product due to the custom nature of some of the schema and the various encryption efforts. That is why it is necessary to receive the password from the user and not the source datastore. The system and method of the present application waits for the approval response from the source user authenticator before populating the target datastore with the password entered by the user as a way of verifying if the identification and password entered by the user are valid, not as a way of restoring missing data.

Neither of the cited references, singly or in any motivated combination thereof, address the problems associated with migrating data from one vendor's proprietary database schema to another vendor's product and do not teach or suggest the solution disclosed in the present

application. Accordingly, Applicants respectfully submit that the teachings of these references would not suggest the claimed subject matter to a person of ordinary skill in the art.

IV. The agency module 112 of Mehring provides an interface for communications between the web server 110 and the policy server 114. It does not intercept a request to the source user authenticator from a user seeking access to information protected by the target user authenticator.

With regard to independent Claim 16, Claim 16 recites, "intercepting a request to the source user authenticator from a user seeking access to information protected by the target user authenticator."

The Office Action appears to suggest that the agency module 112 of Mehring intercepts a request to the source user authenticator from a user seeking access to information protected by the target user authenticator. However, Mehring relates to a method of allowing a remote system user to requests multiple software applications using a single log-in. Mehring does not teach or suggest migrating data from a source datastore to a target datastore. Therefore, it cannot be said that the agency module 112 of Mehring intercepts a request to the source user authenticator from a user seeking access to information protected by the target user authenticator when Mehring does not teach or suggest a source user authenticator or a target user authenticator. Rather, "The agency module 112 provides an interface for communications between the web server 110 and the policy server 114." (Col. 8, lines 6-8.) Providing an interface for communications between a web server and a policy server is not the same thing as intercepting a request to the source user authenticator from a user seeking access to information protected by the target user authenticator.

Accordingly, Applicants respectfully submit that Mehring does not teach or suggest intercepting a request to the source user authenticator from a user seeking access to information protected by the target user authenticator.

Claim 16 also recites, "locating the corresponding identification in the target datastore and determining whether the target datastore includes a password associated with the identification."

The Office Action appears to suggest that the foreign registries of Blakely locate a corresponding identification in their target datastore and determine whether their datastores include a password associated with the identification. However, as stated earlier, it is not necessary for the foreign datastores of Blakely to determine if their datastores include a password

associated with an identification because the datastores of Blakely are configured to be propagated immediately with any changes to passwords in the DCE datastore.

Accordingly, Applicants respectfully submit that Blakely does not teach or suggest locating the corresponding identification in the target datastore and determining whether the target datastore includes a password associated with the identification.

Claim 16 further recites, "if the target datastore does not include a password associated with the identification, then: allowing the original intercepted request to go through to the source user authenticator."

The Office Action does not appear to address this element of Claim 16, and Applicants are unable to find such a teaching in any of the cited references.

Accordingly, Applicants respectfully submit that none of the cited references, singly or in any motivated combination thereof, teaches or suggests that if the target datastore does not include a password associated with the identification, then allowing the original intercepted request to go through to the source user authenticator.

Claim 16 also recites, "on receipt of an approval response from the source user authenticator, populate the target datastore with the received password associating the received password with the corresponding identification."

As stated earlier, the Office Action appears to suggest that the target datastore of the present application is populated from the source datastore. However, for the reasons stated earlier, the target datastores cannot be populated with passwords from the source datastore because simply propagating passwords from one datastore to another is not possible when migrating from one vendor's proprietary database schema to another vendor's product due to the custom nature of some of the schema and the various encryption efforts.

Neither of the cited references, singly or in any motivated combination thereof, address the problems associated with migrating data from one vendor's proprietary database schema to another vendor's product and do not teach or suggest the solution disclosed in the present application. Accordingly, Applicants respectfully submit that the teachings of these references would not suggest the claimed subject matter to a person of ordinary skill in the art.

With regard to independent Claim 19, Claim 19 recites, "intercepting a request to the source user authenticator from a user seeking access to information protected by the target user

authenticator."

The Office Action appears to suggest that the agency module 112 of Mehring intercepts a request to the source user authenticator from a user seeking access to information protected by the target user authenticator. However, as stated earlier, the agency module 112 provides an interface for communications between the web server 110 and the policy server 114. (Col. 8, lines 6-8.) It does not intercept a request to the source user authenticator from a user seeking access to information protected by the target user authenticator.

Accordingly, Applicants respectfully submit that Mehring does not teach or suggest intercepting a request to the source user authenticator from a user seeking access to information protected by the target user authenticator.

Claim 19 also recites, "locating the corresponding identification in the target datastore and determining whether the target datastore includes a password associated with the identification."

The Office Action appears to suggest that the foreign registries of Blakely locate a corresponding identification in their target datastore and determine whether their datastores include a password associated with the identification. However, as stated earlier, it is not necessary for the foreign datastores of Blakely to determine if their datastores include a password associated with an identification because the datastores of Blakely are configured to be propagated immediately with any changes to passwords in the DCE datastore.

Accordingly, Applicants respectfully submit that Blakely does not teach or suggest locating the corresponding identification in the target datastore and determining whether the target datastore includes a password associated with the identification.

With regard to independent Claim 22, Claim 22 recites, "intercepting a request to the source user authenticator from a user seeking access to information protected by the target user authenticator."

The Office Action appears to suggest that the agency module 112 of Mehring intercepts a request to the source user authenticator from a user seeking access to information protected by the target user authenticator. However, as stated earlier, the agency module 112 provides an interface for communications between the web server 110 and the policy server 114. (Col. 8, lines 6-8.) It does not intercept a request to the source user authenticator from a user seeking

access to information protected by the target user authenticator.

Accordingly, Applicants respectfully submit that Mehring does not teach or suggest intercepting a request to the source user authenticator from a user seeking access to information protected by the target user authenticator.

Claim 22 also recites, "locating the corresponding identification in the target datastore and determining whether the target datastore includes a password associated with the identification."

The Office Action appears to suggest that the foreign registries of Blakely locate a corresponding identification in their target datastore and determine whether their datastores include a password associated with the identification. However, as stated earlier, it is not necessary for the foreign datastores of Blakely to determine if their datastores include a password associated with an identification because the datastores of Blakely are configured to be propagated immediately with any changes to passwords in the DCE datastore.

Accordingly, Applicants respectfully submit that Blakely does not teach or suggest locating the corresponding identification in the target datastore and determining whether the target datastore includes a password associated with the identification.

Claim 22 also recites, "if the target datastore does not include a password associated with the identification, then: allowing the original intercepted request to go through to the source user authenticator."

The Office Action does not appear to address this element of Claim 22, and Applicants are unable to find such a teaching in any of the cited references.

Accordingly, Applicants respectfully submit that none of the cited references, singly or in any motivated combination thereof, teaches or suggests that if the target datastore does not include a password associated with the identification, then allowing the original intercepted request to go through to the source user authenticator.

Claim 22 further recites, "on receipt of an approval response from the source user authenticator, capturing the password provided by the user in response to the source authenticator prompting and using the captured password as the received password."

As stated earlier, the Office Action appears to suggest that the passwords of the target datastore of the present application are populated from the source datastore. However, Applicants respectfully submit that this is not what is claimed. What is claimed is populating the

target datastore from the password **provided by the user**, not the source datastore. The reason for using the password provided by the user is that the target datastores cannot be populated from the source datastore. This is because in many security migrations, simply propagating passwords from one datastore to another is highly difficult to impossible when migrating from one vendor's proprietary database schema to another vendor's product due to the custom nature of some of the schema and the various encryption efforts.

Neither of the cited references, singly or in any motivated combination thereof, address the problems associated with migrating data from one vendor's proprietary database schema to another vendor's product and do not teach or suggest the solution disclosed in the present application. Accordingly, Applicants respectfully submit that the teachings of these references would not suggest the claimed subject matter to a person of ordinary skill in the art.

Dependent Claims 2-15, 17, 18, 20, 21, 23, and 24 depend directly or indirectly from independent Claims 1, 16, 19, and 22 and incorporate all of the limitations thereof. Accordingly, for the reasons established above, Applicant respectfully submits that Claims 1-24 are not obvious in light of the suggested combination and respectfully request allowance of these claims.

Conclusion

Applicants respectfully submit that the present application is in condition for full allowance for the reasons stated above, and Applicants respectfully request such allowance. If the Examiner has any questions or comments or feels it would be helpful in expediting the application, the Examiner is encouraged to telephone the undersigned at (972) 731-2288. This correspondence is intended to be a complete response to the Final Office Action dated July 13, 2006. The Commissioner is hereby authorized to charge payment of any further fees associated with any of the foregoing papers submitted herewith, or to credit any overpayment thereof, to Deposit Account No. 21-0765, Sprint.

Respectfully submitted,

Date: 9/5/2006

Michael W. Piper
Reg. No. 39,800

ATTORNEY FOR APPLICANTS

CONLEY ROSE, P.C.
5700 Granite Parkway, Suite 330
Plano, Texas 75024
(972) 731-2288
(972) 731-2289 (facsimile)